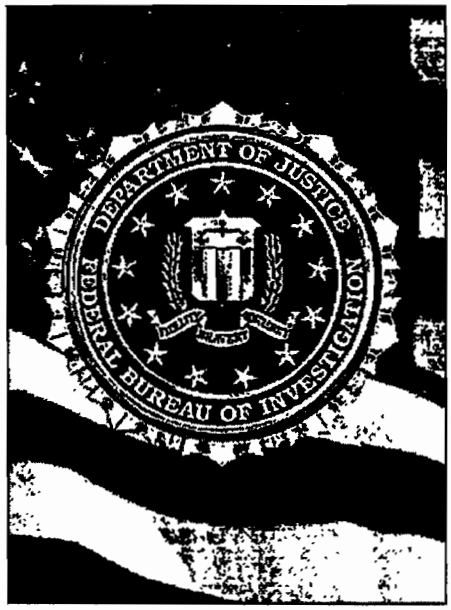
FBI Intelligence Information Report (IIR) Handbook



Federal Bureau of Investigation (FBI)

0083PIG

May 14, 2008

The first two of the following examples would be approved for dissemination as a threat; however, the third example would not be approved for dissemination as a threat.

b2
b7E

4.3.9. Dissemination of Open-Source Information in an IIR

It is not the role of an IIR to provide raw data mined from open sources to the USIC. IIRs provide recipients with raw intelligence they would otherwise not have access to because it has been obtained from FBI sources and/or investigations. As such, the FBI does not routinely disseminate IIRs that report information that is wholly available in open sources. The FBI does, however, add publicly available information to IIRs (particularly via an FBI comment) when doing so provides context to the reporting. Part VII.S of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) defines "publicly available" as information that:

- Has been published or broadcast for public consumption,
- Is available on request to the public,
- Is accessible online or otherwise to the public,
- Is available to the public by subscription or purchase,
- Could lawfully be seen or heard by any casual observer,
- Is made available at a meeting open to the public, or
- Is obtained by visiting any place or attending any event that is open to the public.

As a general rule, if the information could be obtained via a Google search, it should not be reported in an IIR. The following points provide general guidance on common open-source reporting scenarios.

> Some of the reporting is publicly available, but some is not. In this situation, the IIR author should determine whether the nonpublic information is important—whether it is considered intelligence on its own or enhances the open-source reporting in a meaningful way. For example, suppose media outlets are reporting that unidentified individuals have fire-bombed a particular church. If source reporting provides salient details not reported by the media, such as the identity of the perpetrators as white supremacists, the information should be reported in an IIR.

The information was posted online, but it is no longer available. Such information would be appropriate for dissemination in an IIR because it is no longer available to the USIC. The same standard applies to printed information, such as a leaflet, that has been publicly distributed in a limited manner but is no longer available. However, if the information is available via a Web site that archives online content (such as www.archive.org), the information is still considered open-source.

The information is currently publicly available, but the field office initially received the information from an FBI source. In such a situation, it is possible open-source reporting is corroborating source reporting, but it is also possible the source provided the information to the FBI by data-mining the Internet. Regardless of where the information originated, it is not reportable in an IIR if it is currently publicly available.

Source reporting conflicts with open-source reporting. Such information is reportable in an IIR if the discrepancy is of intelligence value *and* if there is reason to believe the source reporting is at least as authoritative as the media.

A threat is posted in an open-access obscure forum or Web site. Such information would not be reportable in an IIR. If a field office finds a threat posted in a forum or on a Web site, it may determine it necessary to set a lead to investigate the potential threat and notify relevant parties. However, the FBI does not routinely use an IIR to disseminate threats presented in open-access media such as personal Web sites, groups' Web sites, Internet forums, MySpace pages or similar sites, or YouTube or similar sites.

The information is available online, but registration and/or a password is required to view it. Technically, such information is considered open-source since it is available online. However, such information is reportable in an IIR if it is accessed as part of an FBI investigation via covert accounts. In this instance, it is considered raw intelligence to which other USIC/law enforcement community members are unlikely to have access.

A threat or other information of interest is publicly available, but it is written in a foreign language. Such information is not reportable in an IIR. The Open Source Center (OSC) is the USIC's designated provider of foreign open-source intelligence. OSC information can be accessed through Intelink-SBU, the USIC's Sensitive But Unclassified information-sharing network.

4.3.10. Dissemination of Grand Jury Information in an IIR

Section 203(a) of the Patriot Act discusses the circumstances under which the FBI has the authority to share certain types of Grand Jury information. For example, §203(a)(1)(C)(i)(V) explains that in general, foreign intelligence or counterintelligence Grand Jury information may be disclosed to federal law enforcement, intelligence, protective, immigration, national defense, or national security officials to assist the officials in the performance of their official duties. An FBIHQ attorney must always be consulted prior to releasing Grand Jury information in an IIR.